12708

Monge, Elaine (SCA)

From: noreply@formstack.com
Sent: Friday, March 23, 2018 4:50 PM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications

Formstack Submission For: Security Breach Notifications

Submitted at 03/23/18 4:50 PM

Business Name:	Squire Patton Boggs (US) LLP
Business Address:	4900 Key Tower, 127 Public Square Cleveland, OH 44114
Foreign Business Address:	
Company Type:	Other
Your Name:	Stacy Ballin
Title:	Partner and General Counsel
Contact Address:	Same as above
Foreign Contact Address:	
Telephone Number:	(216) 479-8500
Extension:	8523
Email Address:	stacy.ballin@squirepb.com
Relationship to Org:	Other

Breach Type:	Paper
Date Breach was Discovered:	01/31/2018
Number of Massachusetts Residents Affected:	9
Person responsible for data breach.:	Current Employee
Please give a detailed explanation of how the data breach occurred.:	Our law firm learned that in the course of mailing out annual Form 1099s, the hard copy of one individual's Form 1099 was mistakenly included in an envelope of another recipient's Form 1099. The Form 1099s contain the Tax ID numbers of corporate payees, or the social security number of individual payees, along with name and mailing address and other information found in a Form 1099. The incident occurred at the end of January 2018, when our firm's accounting staff sent Form 1099s relating to all vendors or other third parties we had paid during 2017 for whom Form 1099s are required. We learned of the incident on February 7, 2018, when a vendor who received two Form 1099s in their package alerted us to the issue involving a New Jersey resident.
Please select the type of personal information that was included in the breached data.:	Social Security Numbers = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The person(s) with possession of personal information had authorized access = Selection(s)
For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information was restricted to authorized personnel only.:	Yes
Network configuration of breached system:	N/A

For breaches involving electronic systems, complete the following:	N/A = Selection(s)
All Massachusetts residents affected by the breach have been notified of the breach.:	Yes
Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::	US Mail = Selection(s)
Date notices were first sent to Massachusetts residents (MM/DD/YYYY):	03/12/2018
All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services .:	Yes
Law enforcement has been notified of this data breach.:	No
Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.:	We consulted with data privacy lawyers and a third party forensic vendor and took steps to identify as best we could who was affected by the error. We took prompt remedial steps, including proper instructions to employees in handling 1099s. We will have enhanced oversight of staff for the future sending of 1099s. Finally, as an additional precaution, we arranged to have AllClear ID protect the identity of the potentially affected individuals for 12 months at no cost to them. The services include identity protection, identity repair, and credit monitoring.

Formstack, 8604 Allisonville Road, Suite 300, Indianapolis, IN 46250

Monge, Elaine (SCA)

From: McKean, Amy L. <amy.mckean@squirepb.com> on behalf of Ballin, Stacy D. <stacy.ballin@squirepb.com>
Sent: Friday, March 23, 2018 5:01 PM
To: Breaches, Data (SCA)
Cc: Ballin, Stacy D.
Subject: Data Breach Notification Submission
Attachments: Data Breach Notification Submission.pdf; Consumer Notice.pdf

Attached please find the Data Breach Notification Submission also submitted online as well as the Consumer Notice, as required.

SQUIRE PATTON BOGGS

Stacy D. Ballin
Partner and General Counsel
Squire Patton Boggs (US) LLP
4900 Key Tower
127 Public Square
Cleveland, Ohio 44114
T +1 216 479 8523
O +1 216 479 8500
F +1 216 479 8780
M +1 216 268 9462

Stacy.Ballin@squirepb.com | squirepattonboggs.com

Mass.gov

Data Breach Notification Submission

Data Breach Notification Submission

Instructions: Please complete the form below to submit a data breach notification to the Office of Consumer Affairs and Business Regulation. You can also print this submission for your own records. Please note under M.G.L. C93H, a separate notification must be sent to the Attorney General's Office.

If you're mailing your submission, please send to: Office of Consumer Affairs and Business Regulation, 501 Boylston St., Suite 5100, Boston, MA 02116

- Individual breaches affecting multiple debit/credit card holders of your organization can be reported on a monthly basis.
- Please do not include any personally identifiable information for Massachusetts residents in any of the fields.

Section I: Organization & Contact Information

Business Name *

Squire Patton Boggs (US) LLP

Business Address (optional)

4900 Key Tower, 127 Public Square

Cleveland

City

Ohio

State

44114

ZIP Code

Foreign Business Address (optional)

If your business is located outside the United States, enter the address here

Company Type *

Other

Your Name *

Stacy

First Name

Ballin

Last Name

Title *

Partner and General Counsel

Contact Address (optional)

Same as above

City

State

ZIP Code

Foreign Contact Address (optional)

If your contact address is outside the United States, enter the address here

Telephone Number *

(216) 479-8500

Extension (optional)

8523

Email Address *

stacy.ballin@squirepb.com

Relationship to Org *

Other

Section II: Breach Information

Breach Type *

Paper

Date Breach was Discovered *

01 31 2018

Number of Massachusetts Residents Affected *

9

Person responsible for data breach. *

Current Employee

Please give a detailed explanation of how the data breach occurred. *

Our law firm learned that in the course of mailing out annual Form 1099s, the hard copy of one individual's Form 1099 was mistakenly included in an envelope of another recipient's Form 1099. The Form 1099s contain the Tax ID numbers of corporate payees, or the social security number of individual payees, along with name and mailing address and other information found in a Form 1099. The incident occurred at the end of January 2018, when our firm's accounting staff sent Form 1099s relating to all vendors or other third parties we had paid during 2017 for whom Form 1099s are required. We learned of the incident on February 7, 2018, when a vendor who received two Form 1099s in their package alerted us to the issue involving a New Jersey resident.

Please select the type of personal information that was included in the breached data.*

	Selection(s)
Financial Account Numbers	☐
Social Security Numbers	☑
Driver's License	☐
Credit/Debit Card Number	☐

Please check ALL of the boxes that apply to your breach.*

	Selection(s)
The person(s) with possession of personal information had authorized access	☑
The breach was a result of a malicious/criminal act.	☐
The breach occurred while the data was being transported outside of your premises.	☐
The breach occurred at the location of a third party service provider.	☐

There is a written contract in place with the third-party provider requiring protection of personal information.	☐

Section III: Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data. *

☐ Yes

☐ No

☑ N/A

Physical access to systems containing personal information was restricted to authorized personnel only. *

☑ Yes

☐ No

☐ N/A

Network configuration of breached system *

N/A

For breaches involving electronic systems, complete the following *

	Selection(s)
Breached data was encrypted.	☐
The key to encrypted data was stolen.	☐

03 12 2018

All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services . *

☑ Yes

☐ No

Law enforcement has been notified of this data breach. *

☐ Yes

☑ No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring. *

We consulted with data privacy lawyers and a third party forensic vendor and took steps to identify as best we could who was affected by the error. We took prompt remedial steps, including proper instructions to employees in handling 1099s. We will have enhanced oversight of staff for the future sending of 1099s. Finally, as an additional precaution, we arranged to have AllClear ID protect the identity of the potentially affected individuals for 12 months at no cost to them. The services include identity protection, identity repair, and credit monitoring.

- Any documents pertaining to the data breach including the letter being sent to the Massachusetts residents must be sent via email to data.breaches@state.ma.us
- Please do not include any personally identifiable information for Massachusetts residents in any email attachment.
- Individual breaches affecting multiple debit/credit card holders of your organization can be reported on a monthly basis.
- Please review the information you have entered and click on the "Submit Form" button below.

SUBMIT FORM

SQUIRE PATTON BOGGS

Squire Patton Boggs (US) LLP
1500 W. 3rd Street, Suite 450
Cleveland, Ohio 44113

O +1 216 687 3400
F +1 216 687 3401
squirepattonboggs.com

Michael E. McKenna
T +1 216 687 3427
michael.mckenna@squirepb.com

[DATE]

[NAME]
[ADDRESS]

Dear _____:

We are writing to inform you of an incident that may have involved your personal information. It has come to our attention that in the course of mailing out annual 1099s, a 1099 for one (1) individual recipient was mistakenly included in the envelope with another recipient's 1099. We are not aware of any other instances where a 1099 recipient received another individual's 1099. To ensure that all intended recipients have received 1099s, we have resent all individual 1099s. In addition, out of an abundance of caution, we are sending letters to all potentially affected individuals (i.e., all individuals who are 1099 recipients) to inform you about the incident and offer credit.

To be clear, we have not learned that your 1099 was mistakenly mailed to another person. However, since we cannot determine whether paper copies of any other individuals' 1099s were mistakenly included in another individual's 1099 envelope, we are notifying all of our individual 1099 recipients, which is why you are receiving this notice.

If you received your 1099 from Squire Patton Boggs (SPB) by the first or second week of February, then your 1099 was not sent to another individual and this notice does not apply to you. If you did not receive your 1099 by the second week in February, it is possible another 1099 recipient received your 1099 along with their own, however it also possible that something else happened, such as, it got lost in the mail, or was opened and misplaced by another person in your household.

For the sake of clarity, no electronic 1099s (or any other electronic records) were affected in this incident.

We want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed Information about Identity Theft Protection.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: _____.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence.

If you have further questions or concerns about this incident, you contact Mike McKenna, Global Chief Financial Officer, Squire Patton Boggs at 216-687-3427. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

Michael E. McKenna
Global Chief Financial Officer
Squire Patton Boggs (US) LLP
1500 W. 3rd Street, Suite 450
Cleveland, Ohio 44113

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

The next 2 paragraphs are regarding incidents involving personal health information. Disregard if not applicable to your situation.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an

Initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- «Time» months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for «Time» months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077